PROTECCIÓN DE DATOS MÉDICOS E INTERNET.

ULISES CORTÉS, JAVIER VÁZQUEZ-SALCEDA Y ANTONIO LÓPEZ-NAVIDAD

"Whatsoever things I see or hear concerning the life of men, in my attendance on the sick or even apart therefrom, which ought not to be noised abroad, I will keep silence thereon, counting such things to be as sacred as secrets".

Hipócrates

La protección de los datos relacionados con la salud de los individuos ha sido una preocupación constante del estamento médico desde el inicio de la práctica de la medicina, como queda reflejado en el famoso juramento de Hipócrates que obliga al médico a conservar el secreto de cuanta información obtienen del paciente durante un tratamiento.

Los cambios en la práctica de la medicina, su institucionalización, la aparición de las historias clínicas como método de almacenamiento de datos importantes sobre el paciente para facilitar tarea del médico, etc., han provocado que a lo largo del tiempo los médicos, las instituciones de salud y, en el último siglo, las industrias relacionadas con la salud –aseguradoras, industrias farmacéuticas, etc.-- hayan desarrollado distintos métodos para procurar el mantenimiento de la privacidad de los datos que obtienen y almacenan de los pacientes[1].

La aparición de los ordenadores, primero como sistemas de almacenamiento de los datos –lo que ha permitido el nacimiento de grandes archivos de información médica-- y luego como sistemas de gestión y compartición de la información, ha provocado una verdadera revolución en el diseño de los métodos necesarios para velar por la seguridad de la información de datos médicos. Y, en medio de toda esa agitación, una segunda ola en esta revolución ha llegado con el advenimiento de Internet como medio de comunicación y compartición de la información médica, incluyendo su impacto en las prácticas médicas (como por ejemplo, la telemedicina).

El uso de tecnologías de la información para codificar los datos médicos, las posibilidades de ligar datos médicos de la población provenientes de diversas fuentes (por ejemplo, las bases de datos de varios centros de salud europeos o las bases de datos médicas islandesas que permiten incluso trazar la historia genética de la población de aquella isla) y el que esta información sea explotada por una empresa fuera del ámbito de la salud (por ejemplo, una compañía de seguros de vida) ha creado recelo entre los usuarios que son, de hecho, los poseedores legales de sus datos personales y que quieren tener un control sobre la difusión de esos datos, sobretodo los datos médicos.

Es posible señalar dos tipos de preocupaciones derivadas del uso de los ordenadores para datos médicos: a) las posibles *fugas o filtrado* de información causados por individuos o por instituciones y, b) el posible desvío de información desde las instituciones de salud hacia terceros para su explotación.

Esto ha dado origen a una infinidad de políticas, prácticas y procedimientos en el tratamiento de la información *ad hoc* que han ido

1 Los términos privacidad, confidencialidad y seguridad son usados de formas muy diversas a la hora de discutir la protección de la información médica de carácter personal. Aquí se utilizará como convención usar el término privacidad para referir el deseo de un individuo a limitar la distribución de la información médica que existe sobre él o ella. Se usará el término confidencialidad para indicar las condiciones en las cuales la información médica sobre personas es compartida y/o distribuida de forma controlada. La seguridad se refiere a las medidas que las organizaciones implementan para proteger la información a su cargo y los sistemas que las albergan. También incluye los esfuerzos para mantener la confidencialidad y asegurar la integridad y la disponibilidad de la información

derivando en estándares *de facto* que luego resultan difíciles de compaginar. Aunque hay que decir que, antes del advenimiento de los ordenadores, la seguridad y la privacidad de los datos médicos era ya un problema de cierta magnitud en las sociedades desarrolladas donde los servicios de salud alcanzan a la mayoría de la población.

Los estados han intentado regular la protección de los datos de tipo personal para evitar, en la medida de lo posible, la difusión y uso indebidos de los mismos.

En el caso que nos ocupa es evidente el crecimiento acelerado del uso de tecnologías de la información y las comunicaciones para comunicar y compartir datos médicos. Hoy el uso de ordenadores está generalizado entre la clase médica pero esta situación debe considerase como reciente y está todavía lejos de ser ideal en el sentido de una utilización óptima de los recursos disponibles. En paralelo a este incremento, existe también un crecimiento en la inversión en equipo informático y software no solo para agilizar el intercambio sino también para asegurar la integridad, confidencialidad y seguridad de la información. Y aunque de momento la transmisión y compartición de la información médica –al menos en el caso español— está restringida a las fronteras impuestas por la red local de una institución, no es difícil prever que esta situación cambiará de forma acelerada cuando las instituciones y centros de salud vean las ventajas de compartir información entre ellas.

Existen esfuerzos muy importantes para poner en práctica un conjunto de políticas que aseguren la protección de los datos médicos en un escenario de uso masivo de computadoras en el sector de la salud. Un ejemplo lo podemos ver en los Estados Unidos de América ante la creación del Health Informatics Standards Board (HISB), dependiente del American National Standards Institute (ANSI). Este organismo debe generar procedimientos para crear 1) estructuras de almacenamiento de datos médicos en formato electrónico; 2) para el intercambio de datos, imágenes, sonidos y señales médicas entre instituciones médicas; 3) códigos y terminología apropiada para la distribución de mensajes con contenido médico, 4) mecanismos de comunicación con instrumentos de diagnóstico y otros equipos que producen información médica; 5) diseñar los mecanismos de comunicación y representación de los protocolos médicos en bases de conocimiento y bases de datos, y 6) mecanismos que aseguren la privacidad, la confidencialidad y la seguridad de la información médica.

Objetivos

Los objetivos principales de este artículo son: 1) analizar la evolución de la legislación, tanto española como europea, sobre protección de datos de carácter personal -y, en particular, de datos clínicos- y 2) proponer mecanismos que permitan al tiempo satisfacer sus requerimientos y facilitar la tarea de una unidad de obtención de órganos y tejidos.

También se discute la oportunidad de utilizar formatos electrónicos para almacenar las historias clínicas como una forma de agilizar la transmisión de información y mejorar la gestión de la misma y incidir así en una mejora del servicio sanitario.

Las ventajas de los formatos electrónicos para los datos médicos

El principal beneficio de implantar y usar formatos electrónicos para compilar las historias médicas de los pacientes reside en agilizar el acceso sobre esos datos y en aumentar el control sobre el acceso a esa información de forma mecánica. Es decir, es posible identificar de forma unívoca a los usuarios autorizados y conocer el alcance de sus privilegios a la hora de acceder a la información, así como mantener un registro de acceso (tal y como lo requiere la ley). Además las historias médicas en formato electrónico permiten, al personal autorizado: 1) acceder desde distintos sitios a la información, 2) compartir la información con otros usuarios autorizados, y 3)que varias personas puedan, si es necesario, acceder de forma concurrente (es decir, al mismo tiempo) a la misma

información.

Estos registros electrónicos permiten la posibilidad de mantener la historia clínica de un individuo a lo largo de su existencia e incluir en ella la medicación actual, resultados de laboratorio e incluso imágenes de todo tipo (radiografías, tomografías, etc.).

Los requisitos que la comunidad médica espera de un soporte electrónico para los datos médicos

El soporte multimedia de los datos médicos de un paciente debe redundar en facilitar la tarea del médico a la hora realizar un diagnóstico. Esto requiere que la especificación de dichos formatos cumpla con un conjunto de requerimientos muy exigente entre los que se incluyen:

1. Expresividad, un médico debe poder plasmar cualquier información que considere relevante y ésta debe integrarse de forma natural con el resto;
2. Flexibilidad, debe permitir que cualquier miembro del personal sanitario pueda manipularlo sin necesidad de tener conocimientos informáticos profundos;
3. Seguridad, debe inspirar confianza a los médicos, los pacientes y, en general, a la sociedad;
4. Robustez, debe soportar posibles ataques o uso inadecuado sin dejar de prestar servicio;
5. Verificable, debe permitir en cualquier momento una auditoría que valide la consistencia de la información contenida en el sistema;
6. Reusable, la información sobre un paciente generada en un servicio o en un centro de salud de poder integrarse de forma natural en las bases de datos de otro.

Los requisitos impuestos por la ley: la legislación vigente sobre protección de datos de carácter personal

Los datos médicos tales como el historial clínico de un paciente son considerados por la legislación vigente como uno de los tipos de datos personales que requieren de mayor protección.

La preocupación por la influencia que la informática podía tener en la intimidad de las personas ha llevado a muchos países a la creación de normativas al respecto. En el caso de España el control legislativo de la informática se introdujo desde el primer momento en la Constitución Española, que en su artículo 18.4 emplaza al legislador a limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos.

Pero la Constitución Española sólo contemplaba la intimidad, no la privacidad. En la legislación española se entiende por privacidad un conjunto más amplio de facetas de la personalidad de un individuo que, consideradas por separado pueden no tener ningún valor o significado intrínseco pero que, al unirlas de forma coherente, pueden generar retratos o perfiles de la personalidad del individuo. Precisamente con el objetivo de proteger la privacidad se desarrolló la Ley orgánica 5/1992 (más conocida como LORTAD [5]), que establece la mencionada definición del concepto de privacidad y después establece toda una normativa sobre 1) los ficheros de datos[2] que poseen información de individuos[3], 2) su posible tratamiento y uso, ya sea automatizado o no, por parte de entidades publicas o privadas, 3) las obligaciones relativas a la calidad de los datos, la seguridad técnica y a la notificación a una autoridad de control[4], y 4) los derechos de las personas a acceder a esos datos, solicitar su rectificación o

2 Se entiende por fichero de datos todo tipo de soporte físico de información, ya sea en soporte informático (ficheros informáticos, bases de datos), en papel, en microfilms, etc.

3 Una persona física, completamente identificada en esos datos o identificable a partir de ellos. Nos referiremos a esa persona como el *interesado* o el *afectado*.

4 La Agencia de Protección de Datos, creada a partir de la LORTAD.

incluso oponerse a su tratamiento.

Se consideran datos personales aquellos que permiten identificar a una persona y que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como los datos relativos a la salud o la sexualidad. Por lo tanto, los datos médicos se encuentran al amparo de esa Ley Orgánica.

La LORTAD, incluida su ampliación por el Real Decreto 1333/1994 [6], establece las siguientes normas generales:

1. Calidad de los datos: los datos deben de ser exactos y estar actualizados. Esta norma no supone ningún problema en el caso de datos médicos, que por su naturaleza deben ser correctos en todo momento.
2. Avisar a la persona de sus derechos ante la información recogida: los afectados a los que se les soliciten datos deberán ser informados a) de que sus datos serán introducidos en un fichero, b)del tratamiento que se hará a estos datos, c) del derecho a acceder, rectificar, cancelar o oponerse a la recogida de esos datos, y d) de la identidad y dirección del responsable del tratamiento de los datos, al que se podrán dirigir. En el caso de datos médicos esta norma se ve modificada por el artículo 8 de la misma LORTAD, donde se da automáticamente permiso a las instituciones y centros sanitarios, sean públicos o privados, para obtener y tratar información de los pacientes que acudan o que sean tratados, de acuerdo con lo dispuesto en leyes como la Ley General de Sanidad (LGS [2]), la Ley del Medicamento [4] o la Ley Orgánica 3/1986 [3]. Por poner un ejemplo de modificación que estas leyes anteriores producen, según la LGS no es necesario el consentimiento del paciente a la obtención de datos para su tratamiento cuando la no intervención ponga en peligro la Salud Pública, o bien cuando la urgencia no permita demoras en el tratamiento por poderse producir lesiones irreversibles o existir peligro de fallecimiento.
3. Consentimiento del afectado: como norma general, el tratamiento de los datos de carácter personal requiere el consentimiento de la persona afectada. Al igual que en la norma anterior, en el caso de los datos médicos se modifica esta norma, siguiendo leyes específicas como la LGS.
4. Comunicación de datos: los datos solo pueden ser cedidos o comunicados a terceras personas o instituciones si es para cumplir con los fines para los que se recogieron los datos y si la o las personas afectadas han consentido esta cesión. En el caso de datos médicos el artículo 8 antes citado da permiso de tratamiento a cualquier institución o centro de salud, sea público o privado, por lo que la cesión de datos se puede hacer a cualquier institución o centro de salud en los casos contemplados en el artículo 11: no se necesita consentimiento del afectado (el paciente) a la hora de hacer una cesión de datos referentes a al salud cuando dicha cesión sea necesaria para solucionar una urgencia que requiera acceder a un fichero automatizado o bien para poder realizar estudios epidemiológicos, según establece el artículo 8 de la LGS. De forma similar el artículo 33 de la LORTAD permite la cesión internacional de datos entre facultativos o instituciones sanitarias.
5. Seguridad de los datos: se deben de adoptar medidas técnicas y organizativas para garantizar la seguridad de los datos de carácter personal, evitando su tratamiento o acceso no autorizados, su alteración indebida o bien su pérdida irrecuperable. Las medidas de seguridad a aplicar se especificaron mediante el Real Decreto 994/1999 [12], del que hablaremos más adelante.
6. Notificación a la Agencia de Protección de Datos: la creación de cualquier fichero o soporte físico de datos personales ha de ser notificada a la Agencia de Protección de Datos. La notificación debe especificar, entre otras cosas: quien es el responsable del fichero, objetivo de esos datos, la estructura que se utilizará para almacenarlos, los tratamientos que se realizaran sobre ellos y las cesiones de datos que se prevean. En base a esa notificación la Agencia de Protección de Datos autorizará la creación del fichero de datos.

También se ha de notificar toda modificación en la estructura de los datos, y la primera cesión de datos que se haga.

Hacia 1994 España no era el único estado con una legislación al respecto. La Unión Europea (a diferencia de los Estados Unidos) había manifestado una especial preocupación por la protección de la intimidad de los datos personales de sus ciudadanos. En 1995 ya había varios estados con legislaciones que versaban sobre el tratamiento de datos personales. Sin embargo, dichas legislaciones impedían el intercambio de información sobre personas entre países. El Parlamento Europeo creó la Directiva 95/46/CE [8] con el fin de homogeneizar la cobertura legal sobre protección de datos para garantizar un nivel adecuado de protección en toda transferencia dentro de la Unión Europea. Dicha directiva[5] no aportó grandes modificaciones en el marco legal español, que ya tenía una ley muy protectora, pero si aportó algunos matices y normativas que se añadieron con posteridad a la nueva redacción de la ley sobre protección de datos, la Ley orgánica 15/1999 [14].

Las modificaciones introducidas por la directiva europea son las siguientes:

1. Ampliación del ámbito: se extiende el ámbito de aplicación de la legislación a todo fichero de datos estructurados de forma que se pueda extraer información de personas fácilmente, independientemente de que se vaya a realizar algún tipo de tratamiento automatizado de la información.
2. Calidad de los datos: solo se pueden guardar datos que permitan la identificación de los interesados durante el periodo necesario para los fines para los que fueron recogidos o las ampliaciones de esos fines que hayan sido autorizadas. En caso de querer guardar esa información más allá de dicho periodo (para fines históricos, estadísticos o científicos), se ha de hacer de forma que no se pueda identificar a los interesados. En el caso de datos médicos los límites permitidos están establecidos en la Recomendación R(97)5 [9], de la que hablaremos más adelante.
3. Excepción a la prohibición de tratamiento en el caso de datos médicos: el artículo 8.3 permite el tratamiento de datos personales "cuando resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto a secreto profesional, sea en virtud de la legislación nacional o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto".
4. Cesión de datos: Los estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los estados miembros por motivos relacionados con el nivel de protección garantizada, puesto que la directiva esta homogeneizando el nivel de protección en toda la Unión Europea. En el caso español esta norma afectó poco, ya que en la Orden de 2 de febrero de 1995 [7], que definía por primera vez la lista de países con normativa de protección de datos equiparable a la española, Italia y Grecia eran los únicos países de la UE a los que no se permitía la cesión de datos, por carecer de leyes sobre protección de datos hasta el año 1996 y 1997. La Orden de 31 de Julio de 1998 [11] ya los incluyó en la lista.
5. Seguridad de los datos: a diferencia de la LORTAD, donde la obligación de velar por la seguridad recae únicamente en el responsable del fichero de datos, la directiva contempla que el responsable del tratamiento de los datos también tenga que velar por la seguridad de los mismos, aplicando todas las medidas que sean necesarias.

5 A finales del año 2000 el Parlamento Europeo amplió la normativa sobre datos personales iniciada por esta directiva mediante el Reglamento (CE) 45/2001 [15], que recoge todo lo ya establecido por la directiva 95/46/CE, precisa el mecanismo de sanciones a nivel europeo e instituye la figura del Supervisor Europeo de Protección de Datos como autoridad de control independiente.

Todas las modificaciones que acabamos de mencionar fueron incorporadas posteriormente en la Ley Orgánica 15/1999 (más conocida como LOPD), una ley que substituye completamente a la LORTAD de 1992, para adaptarla a los nuevos supuestos contemplados por las directivas europeas.

Aparte de las modificaciones ya mencionadas, la LOPD añade los siguientes cambios:

1. Fuente de los datos: se distingue entre fuentes de datos de acceso público o no. Son fuentes de datos de acceso público aquellas que pueden ser consultadas por cualquier persona, ya sea pagando o no, pero sin que exista ningún tipo de norma legal que lo impida. Son ejemplos de fuentes de datos de acceso público los listines telefónicos, los diarios y medios de comunicación o el Boletín Oficial del Estado. En el caso de fuentes como libros u otros soportes físicos, los datos obtenidos perderán el carácter de públicos ante la aparición de una nueva edición. En el caso de información obtenida de forma telemática (por ejemplo, información obtenida en Internet), los datos obtenidos pierden el carácter de públicos pasado un año de la fecha de obtención.
2. Excepción en la notificación al interesado: cuando los datos que se utilizan provienen de una fuente de datos de acceso público no es necesario notificar al interesado del tratamiento que se realizará con esa información.
3. Derecho a oponerse al tratamiento: en los casos en los que no es necesario el consentimiento del interesado para el tratamiento, éste puede oponerse a dicho tratamiento si no hay ninguna ley que disponga de lo contrario.
4. Deber de Notificación: se considera una infracción grave de la ley el no remitir a la Agencia de Protección de Datos las notificaciones establecidas por la ley, como la de notificar antes de la creación de cualquier fichero de datos personales.
5. Cesión nacional de datos: se permite la cesión de datos a terceros si se realiza previamente un proceso de disociación que impida identificar personas concretas.
6. Cesión internacional de datos: la Agencia de Protección de Datos deberá de ser informada antes de realizar la primera cesión de datos a un cierto país. La Agencia será la que determine si el país destinatario posee el nivel de protección adecuado para que se pueda realizar la cesión.

La privacidad y seguridad de los datos médicos en formato electrónico

Una cosa que parece mundialmente aceptada, o al menos en occidente, es la necesidad de proteger la información médica sobre las personas. En Estados Unidos, a falta de leyes que protejan todo tipo de datos personales, se están creando las regulaciones concretas que afectan a la información clínica. Estas regulaciones parten de las recomendaciones expresadas en la Health Insurance Portability and Accountability Act de 1996. Después de un proceso muy largo se ha definido el Reglamento de Privacidad (Privacy Regulation [30]), que teóricamente entra en vigor en febrero del 2001, aunque en muchos casos se da un plazo de 2 a 3 años para adaptarse al reglamento.

En el caso de los estados europeos los datos médicos ya están cubiertos por la Directiva 95/46/CE, por lo que podría parecer innecesario el definir leyes adicionales. Aún así, en 1997 se redactó la Recomendación R(97)5 [9] sobre datos médicos, que substituía completamente a una recomendación anterior de 1981. Dicha recomendación surgió básicamente por dos motivos: 1)se percibía que el progreso de la ciencia médica depende, en buena medida, de la disponibilidad de datos médicos sobre individuos, y 2) se detectó un incremento del uso de datos médicos tratados de forma automática por sistemas de información, no sólo para la asistencia y la investigación médicas, la gestión hospitalaria y la salud pública, sino también fuera del sector sanitario, lo cual era motivo de preocupación.

La R(97)5 no modifica casi las normas que ya hemos visto, puesto que básicamente traduce las

normas de la Directiva 95/46/CE al lenguaje de los datos clínicos y, en algunas normas, precisa los limites de lo que se puede o no se puede hacer para el caso particular de datos médicos. Algunas de las precisiones que introduce son las siguientes:

1. Recogida y tratamiento: la R(97)5 permite la recogida y tratamiento de datos médicos en lo siguientes casos: a)por razones de salud pública; b)para fines médicos preventivos o para fines diagnósticos o terapéuticos relativos al afectado o a un pariente en línea genética (en este caso se permite el tratamiento de esos datos para ofrecer un servicio médico positivo para el paciente); c)para establecer, ejercitar o defender una reclamación legal; y d)para la represión de un crimen específico u otro interés público importante.
2. Derechos de acceso y rectificación del afectado: el acceso del afectado a sus datos médicos puede ser denegado, limitado o rechazado solo si lo prevé la ley y en los siguientes supuestos: a)por razones de seguridad del Estado, seguridad pública o la represión de crímenes, b)el conocimiento de algunos datos puede causar un serio daño a la salud del afectado; c)la información sobre el afectado revela también información sobre otras personas (por ejemplo, parientes consanguíneos o próximos genéticamente); d)los datos son usados con fines científicos o estadísticos y se aprecia con nitidez que no hay riesgo de violación de la intimidad.
3. Derecho de cancelación del afectado: el afectado debe de ser informado de la posibilidad, si existe, de negar su consentimiento a la recogida y tratamiento de sus datos médicos, o de retirar un consentimiento ya dado, y de las consecuencias que esta cancelación puede tener
4. Conservación: solo se pueden conservar datos médicos por más tiempo del necesario para el propósito original con el que se recogieron: a) por un interés legítimo de la salud pública o de la ciencia médica; b) para permitir, a la persona a cargo del tratamiento médico o al controlador del archivo, la defensa ante una reclamación legal; c) por razones históricas o estadísticas (en este caso se han de adoptar las medidas para mantener la intimidad del paciente).

En la ley española no hay ninguna norma adicional sobre datos médicos, pero organismos como el Insalud han redactado normativas internas para sus empleados sobre el uso adecuado de los datos médicos [10].

Medidas de seguridad a seguir en un sistema con información médica.

Como ya se ha mencionado con anterioridad, los datos con información médica son, ante las legislaciones española y europea, datos personales. Por ello, en los sistemas que procesan datos médicos como historiales clínicos, histología, etc. son aplicables todas las medidas de seguridad del Real Decreto 994/1999 [12], el cual ya incluye todas las medidas mencionadas en la Recomendación R(97)5.

En el reglamento de dicho Real Decreto se establecen las medidas mínimas de seguridad de los soportes físicos de la información, estableciendo tres niveles de seguridad según el tipo de información:

- nivel alto: se aplica a ficheros que contengan datos sobre ideología, religión, creencias, origen racial, salud o vida sexual, o bien datos obtenidos para fines policiales sin consentimiento de las personas afectadas
- nivel medio: se aplica a ficheros con datos sobre infracciones administrativas o penales, Hacienda Pública, servicios financieros o información sobre la solvencia patrimonial y crédito.
- nivel básico: aplicable al resto de ficheros de datos personales.

Por lo tanto, los datos médicos se encuentran tipificados en el nivel más alto de exigencias de seguridad, lo cual implica que se tienen que tomar todas las medidas técnicas y de organización, aplicables y adecuadas, para cumplir los siguientes principios:

1. Identificación de usuarios: es imprescindible

introducir mecanismos de identificación[6] y autenticación[7] de las personas e instituciones autorizadas a acceder y/o usar todos o parte de los datos.
2. Control de entrada a las instalaciones: se ha de impedir que cualquier persona no autorizada tenga acceso a las instalaciones donde se guardan o procesan datos personales.
3. Control del soporte de los datos: se ha de impedir que el soporte de datos sea leído, copiado, alterado o retirado por personas no autorizadas.
4. Control de memoria y transmisiones telemáticas: impedir la introducción no autorizada de datos en el sistema de información, así como cualquier consulta, modificación o borrado no autorizado de datos mientras se encuentran en la memoria del o los ordenadores que forman el sistema de información, o mientras estos datos son transmitidos telemáticamente de un ordenador a otro.
5. Control de uso: se han de proteger los datos contra todo tipo de tratamiento no autorizado, incluidas la alteración y la comunicación no autorizadas de dichos datos.
6. Diseño del sistema: por norma general el diseño de la estructura de los datos, de los procedimientos y los accesos selectivos permitidos debe ser tal que permite la separación de a) identificadores y datos relativos a la identidad de las personas, b) datos administrativos, c) datos médicos, d) datos sociales, y e) datos genéticos.
7. Protección ante pérdidas: se han de tomar todas las medidas técnicas y de organización adecuadas para proteger los datos contra su destrucción accidental o ilegal y su pérdida accidental.
8. Recuperación de datos: el sistema ha de tener un correcto sistema de copias de seguridad, y se deben de tener definidos de antemano los procedimientos para la recuperación de los datos en caso de destrucción o pérdida, parcial o total, de los datos.
9. Registro de accesos e introducción de datos: se ha de garantizar que sea posible comprobar y establecer a posteriori cuándo y quién ha accedido al sistema y que información se ha introducido.
10. Registro de incidencias: es obligatorio llevar un registro de todas las incidencias que ocurran, ya sean intentos de acceso no autorizado, fueran exitosos o no, fallos del sistema que necesitaron utilizar las copias de seguridad, etc.

Características que debe tener un Sistema de Información Distribuido con datos médicos.

La tecnología actual permite exigir niveles de seguridad, privacidad y confidencialidad suficientes como para hacer plausible pensar en un uso generalizado y seguro de la información médica relativa a pacientes en formato electrónico. Esto es también posible aún y cuando el sistema en el que se esté pensando esté distribuido en una red local o tenga acceso desde Internet.

Un sistema así debe proveer las siguientes funcionalidades:

1. Disponibilidad: el sistema debe asegurar que la información disponible es precisa y la más actual. Además debe asegurar que dicha información llegará en perfectas condiciones al usuario que la demanda y que toda petición estará supervisada para confirmar su validez.
2. Control de acceso: el sistema debe permitir el acceso total o parcial a los datos según el nivel de autorización de la persona o institución que intenta acceder.
3. Identificación del perímetro: El sistema debe conocer los límites físicos y lógicos del tipo de accesos que debe permitir y evitar accesos fuera de estos límites o sospechosos.

En el caso del control de acceso, como ya hemos visto, dicho control se ha de realizar en varios niveles:

1. Acceso a las instalaciones: se ha de controlar la entrada a todas las instalaciones que tienen máquinas que formen parte del sistema, ya sea mediante sistemas electrónicos de acceso,

6 Procedimiento de reconocimiento de la identidad del usuario

7 Procedimiento de comprobación de la identidad del usuario.

alarmas, la contratación de un servicio de seguridad, etc.

2. Acceso telemático: se han de establecer las medidas de seguridad de redes existentes (como los *firewalls)* para proteger a los ordenadores que estén conectados telemáticamente con el exterior de cualquier acceso telemático no autorizado.
3. Identificación y autenticación del usuario: el nivel mínimo de autenticación se consigue mediante el uso de claves de acceso (de forma habitual un nombre o código de usuario seguido de una palabra-llave o *password*). Pero existen ya en la actualidad medidas aplicables para aumentar el nivel de identificación y autenticación, ya sea en el acceso directo (*in situ*) a las instalaciones y máquinas (tarjetas con banda magnética, tarjetas con chip, reconocedores de voz, reconocedores de retina, etc) o en el acceso telemático (utilización de certificados y firmas digitales).
4. Acceso a los datos en la memoria del ordenador: el control en este caso consiste en tener para cada ordenador, un sistema operativo que realice una buena gestión de la memoria (sobretodo si es compartida entre varios usuarios).
5. Acceso a los datos almacenados: para evitar el obtener información mediante una simple copia de los datos tal cual estos se guardan en los soportes físicos, aparte del control de acceso es recomendable (aunque no imprescindible) que los datos sean guardados de forma que no se puedan "leer" directamente. La técnica más habitual es la encriptación de los datos. Se puede optar por a) la encriptación de todos los datos, de forma que son totalmente ilegibles si no se tiene la clave de desencriptado, o bien b) la encriptación de la parte de los datos que permite la identificación de individuos (nombres, documentos de identidad, etc..) y la parte de los datos que guarda las claves de acceso (las palabras-llave o *passwords*), de forma que solo es legible un conjunto de información anónima, sin posibilidad de ser vinculada a ninguna persona identificable.
6. Acceso a los datos durante la comunicación telemática[8]: en el caso de que el sistema este distribuido en varias máquinas y que estas se comuniquen entre ellas datos médicos de forma telemática, es imprescindible evitar que dichos datos sean leídos por alguien no autorizado que los "capture" en su paso por la red telemática. Esto es especialmente importante si se utilizan redes telemáticas que están fuera de nuestro control, como Internet, redes en las que no podemos evitar la captura, accidental o intencionada, de transmisiones de datos. En este caso la técnica más utilizada es la encriptación, pero existen diversas variantes: encriptación por clave privada, encriptación por combinación de clave pública y privada, encriptación con certificados y firmas digitales[9], etc.

Los nuevos usuarios de los datos médicos

Las grandes cantidades de información generadas en un acto médico y la necesidad de relacionar esta información con otra disponible del mismo paciente o de integrarla en bases de datos que permitan extraer conclusiones de una población mayor han supuesto la aparición de nuevos actores. Estas organizaciones proveen nuevos servicios y productos al sector médico cuya existencia y éxito depende, en gran medida, del acopio y uso de información relacionada con los pacientes. Algunos ejemplos son los proveedores de material médico, las empresas farmacéuticas, los laboratorios de referencia, las empresas que proveen sistemas de información, las aseguradoras, etc.

Además la alianza entre algunas de estas organizaciones permite la agregación de datos a

8 La aparición de redes como Internet, donde la seguridad de la información que pasa a través esta siempre en entredicho, y su posible uso para comunicar datos personales ha hecho que el Parlamento Europeo esté preparando, desde agosto de 2000, una propuesta de directiva comunitaria [16] que regule la protección de los datos personales en las comunicaciones electrónicas

9 Las firmas electrónicas estan reguladas desde el Real Decreto-Ley 14/1999 [13].

mayor escala aumentando de forma dramática su valor, no sólo desde el punto de vista informático sino también desde el punto de vista económico. Y es esta característica la que los convierte en objetivo de posibles ataques[10] para aquellos que buscan información.

CONCLUSIONES

La privacidad de los datos médicos es un derecho irrenunciable de los individuos que debe tenerse en cuanta a la hora de la explotación de los datos médicos en formato electrónico, explotación que, por otra parte, representa en sí misma un avance de las posibilidades de ofrecer mejores servicios a los pacientes. Las historias médicas en formato electrónico ofrecen una imagen más exacta del paciente, facilitando la tarea del médico. Es pues importante que los usuarios conozcan las ventajas que ofrecen estos formatos para su propio beneficio, las condiciones de seguridad que la tecnología y la ley ofrecen y, además, los límites de ambas.

Los mecanismos de protección de la información médica deben contemplar y balancear la necesidad de información por parte de los prestadores del servicio con la confidencialidad debida al receptor del servicio.

Esta claro que son las propias organizaciones quienes han de autorizar e identificar a los usuarios –individuos o instituciones-- que han de acceder a las bases de datos que contienen información sobre sus pacientes y también controlar los casos en los que éste acceso estará permitido.

❖ BIBLIOGRAFÍA ❖

1. Ley 30/1979, de 27 de octubre, de la Jefatura del Estado, sobre extracción y trasplante de órganos. BOE[11] núm. 266, de 6 de noviembre de 1979.

2. Ley 14/1986, de 25 de abril, General de Sanidad. BOE núm. 102, de 29 de abril de 1986.

3. Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública. BOE núm. 102, de 29 de abril de 1986.

4. Ley 25/1990, de 20 de diciembre, del Medicamento. BOE núm. 306, de 22 de diciembre de 1990.

5. Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de caracter personal. BOE núm. 262, 31 de octubre de 1992.

6. Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los datos de carácter personal. BOE núm. 147, de 21 de junio de 1994.

7. Orden de 2 de febrero de 1995 por la que se aprueba la primera relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos. BOE núm. 35, de 10 de febrero de 1995.

8. Directiva 95/46/CE del Parlamento Europeo y el Consejo de la Unión Europea, 24 de octubre de 1995. DO[12] L 281, de 23 de noviembre de 1995

9. Recomendación R(97)5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre Protección de Datos Médicos.

10 En el mundo de la seguridad informática se entiende por ataque un acceso no autorizado a un ordenador y a los datos que contiene.

11 Boletín Oficial del Estado.

12 Diario Oficial de las Comunidades Europeas.

10. Instrucciones del Insalud sobre seguridad y protección de datos. Circular núm. 9/97, de 9 de julio de 1997.

11. Orden de 31 de julio de 1998 por la que se amplía la relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos. BOE núm 106, de 21 de agosto de 1998.

12. Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. BOE núm. 151, de 26 de febrero de 2000.

13. Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica. BOE núm. 224, de 18 de septiembre de 1999.

14. Ley Orgánica 15/1999 de Protección de Datos de carácter personal. BOE núm 298, 13 de diciembre de 1999.

15. Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. DO L 8, de 12 de enero de 2001.

16. Propuesta de Directiva del Parlamento Europeo y del consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Presentada por la Comisión el 25 de agosto de 2000.

17. Organización Nacional de Trasplantes (ONT). Donación y trasplante. España 1994. Madrid 1995.

18. Organización Nacional de Trasplantes (ONT). Actividad de donación y trasplante. España 1995. Madrid 1996.

19. T. Alsinet, R. Béjar, C. Fernàndez y F. Manyà (2000) "A Multi Agent System Architecture for Monitoring Medical Protocols. Proceedings of the Fourth International Conference on Autonomous Agents. C. Sierra & M. Gini J. Rosenschein (eds), pp 499-505", ACM-AAAI.

20. F.S. Brightbill (1999) Corneal surgery: Theory, techniques and tissue. Mosby Inc.

21. Computer-based Patient Record Institute (1995) Guidelines for Establishing Information Security Policies at Organizations Using Computer-based Patient Record Systems. CPRI, Schaumburg, Ill., February.

22. U. Cortés, A. López-Navidad, J. Vázquez-Salceda, A. Vázquez, D. Busquets, M. Nicolás, S. Lopes, F. Vázquez y F. Caballero (2000) "Carrel: An Agent Mediated Institution for the Exchange of Human Tissues among Hospitals for Transplantation". 3er Congrés Català d'Intel.ligencia Artificial, pp. 15-22. ACIA.

23. J. Fox, N. Johns, A. Rahmanzadeh y R. Thompson. (1996) "PRO*forma*: A method and a language for specifying clinical guidelines and protocols". Medical Informatics Europe'96. J Brender, J P Christensen, J-R Scherrer and P McNair (Eds). pp516-520".

24. S. García-Sousa, A. López-Navidad, F. Caballero y M.A. Viedma (1999) "Potential Cornea Donors in a General Hospital". Transplantation Proceedings. Vol. 32, pp 2607-2608.

25. López-Navidad, J. Kulisevsky y F. Caballero (1997) El donante de órganos y tejidos: Evaluación y manejo. Springer-Verlag Ibérica. 1 edición.

26. López-Navidad (1997) "Professional Characteristics of the Transplant Coordinator".

Transplantation Proceedings # 23, pp. 1607—1613

27. R. Matesanz (1999) "Meeting the organ shortage: Current status and strategies for improvement of organ donation". Newsletter Transplant. 4(1):5-17.

28. Organización Nacional de Transplantes. (2000) Informes y Documentos de Consenso promovidos por la Organización Nacional de Transplantes y la Comisión de Transplantes del Consejo Interterritorial del Sistema Nacional de Salud. Ed. Complutense S. A.

29. Rector, S. Bechhofer,C.A. Goble, I. Horrocks, W.A. Nolan y W.D. Solomon. (1997) "The GRAIL concept modelling language for medical terminology", *Artificial Intelligence in Medicine*, Vol. 9, pp139-171

30. Eurotransplant. http://www.transplant.org.

31. The National Eye Institute. (NEI). http://www.nei.nih.gov

32. Health Level Seven (HL7). http://www.hl7.org

33. Health Insurance Portability and Accountability Act of 1996. http://www.hcfa.gov/medicaid/hipaa/

34. Veazie, S. (1998) Computer-Based Patient records can accelerate software component commerce. *Journal of Healthcare Information Management. 122(4):21-28*